DELL Technologies

DDoS: versterking van cyberbeveiliging en veerkracht met Dell Technologies

Toenemende dreiging van DDoS-aanvallen

DDoS-aanvallen (Distributed Denial of Service) zijn uitgegroeid tot een van de meest wijdverbreide en verstorende bedreigingen in het digitale tijdperk. Bij DDoS-aanvallen worden enorme netwerken van gecompromitteerde apparaten ingezet om doelsystemen, servers of netwerken te overspoelen met een overweldigende hoeveelheid verkeer. Deze aanhoudende vloedgolf vertraagt activiteiten of brengt ze tot stilstand, waardoor een bedrijf vaak verlamd raakt.

Geen enkele organisatie - van start-up tot multinational - is immuun voor het toenemende aantal DDoS-aanvallen. Naarmate bedrijven steeds afhankelijker worden van een digitale infrastructuur, hebben deze aanvallen verwoestende gevolgen, variërend van financieel verlies tot reputatieschade. Dell Technologies erkent het belang van deze uitdaging en levert schaalbare, innovatieve oplossingen waarmee bedrijven hun verdediging kunnen versterken en de storm kunnen weerstaan.

Wat zijn DDoS-aanvallen?

Bij een DDoS-aanval wordt geprobeerd de normale werking van een netwerk, service of server te verstoren door deze te overweldigen met een enorme vloedgolf aan verkeer vanuit meerdere bronnen. Deze aanvallen worden uitgevoerd door botnets. Dit zijn netwerken met geïnfecteerde apparaten die op afstand door aanvallers worden beheerd.

Hoe DDoS-aanvallen werken

1. **Rekrutering voor een botnet:** cybercriminelen infecteren duizenden of miljoenen apparaten met malware en vormen zo een botnet dat kan worden gemobiliseerd voor een aanval waardoor uw bedrijf onbruikbaar wordt.
2. **Overbelasten met verkeer:** aanvallers zetten botnets in om een overvloed aan aanvragen naar de doelserver te sturen, waardoor het systeem vertraagt, crasht of niet meer beschikbaar is voor legitieme gebruikers.
3. **Systeemoverbelasting:** het systeem, dat wordt overweldigd door onnodig verkeer, kan niet meer voldoen aan legitieme aanvragen, wat resulteert in verstoring van de dienstverlening of ernstige vertragingen.

Veelvoorkomende technieken

- **Bij volumegebaseerde aanvallen** ontstaat er een enorme hoeveelheid verkeer om de bandbreedte van een netwerk volledig te bezetten.
- **Bij protocolaanvallen** worden beveiligingslekken in protocollen misbruikt, zoals TCP/IP, om resources te gebruiken.
- **Aanvallen op applicatielaag** richten zich op specifieke applicaties, zoals een website of database, om de functionaliteit te verstoren.

Deze aanvallen ontwikkelen zich voortdurend, waardoor ze een enorme uitdaging vormen voor bedrijven die hun activiteiten proberen te beschermen.

De impact op bedrijven

Financiële gevolgen

Eén DDoS-aanval kan miljoenen dollars kosten aan inkomsten, downtime en herstelwerkzaamheden. Zelfs enkele minuten waarin een service niet beschikbaar is, kunnen een aanzienlijke impact hebben op bedrijven die afhankelijk zijn van realtime transacties, zoals e-commerceplatforms en financiële dienstverleners.

Operationele verstoring

Onderbrekingen die worden veroorzaakt door een DDoS-aanval verminderen de productiviteit, vertragen kritieke processen en belemmeren de toegang tot essentiële services. Voor sectoren zoals de gezondheidszorg of de productiesector kan operationele downtime verstrekkende gevolgen hebben.

Reputatieschade

Wanneer klanten of cliënten serviceonderbrekingen ervaren, neemt hun vertrouwen af. Langdurige of herhaalde incidenten kunnen leiden tot langdurige schade van de reputatie van een organisatie, wat leidt tot verlies van klanten en minder vertrouwen in de markt.

Praktijkvoorbeeld

In 2020 vond er een opvallend incident plaats, toen een grote financiële instelling het slachtoffer werd van een aanhoudende DDoS-aanval waarbij online bankdiensten enkele uren waren uitgeschakeld. De directe omzetverliezen, in combinatie met een beschadigde reputatie, resulteerden in schadevergoedingen van meer dan **$ 50 miljoen.**

Alarmerende statistieken

Uit het DDoS Insights Report (februari 2024) van Zayo Group blijkt dat de schade bij niet-beschermde organisaties gemiddeld **$ 6000** per minuut bedroeg, wat leidde tot een gemiddelde schadepost van ongeveer **$ 408.000** per incident in 2023. Bovendien neemt het aantal van dergelijke aanvallen toe. Er worden **jaarlijks meer dan 10 miljoen aanvallen gemeld**. Uit deze statistieken blijkt dat er dringend behoefte is aan robuuste preventiemaatregelen.

20,5 miljoen

DDoS-aanvallen geblokkeerd in het 1e kwartaal van 2025

Bron: 2024: Cloudflare DDoS Threat Report

DDoS-aanvallen bestrijden met Dell Technologies

Dell Technologies biedt een geavanceerde suite van oplossingen zodat bedrijven zich kunnen voorbereiden op DDoS-incidenten, deze kunnen detecteren en ervan kunnen herstellen.

Versterkte eindpunten met Dell Trusted Devices

Eindpunten zijn cruciale toegangspunten voor DDoS-gerelateerde bedreigingen. Dell Trusted Devices bieden robuuste beveiligingsfuncties die zijn ingebouwd in de hardware, zoals Secure BIOS en SafeID, die bescherming bieden tegen onbevoegde toegang en de systeemintegriteit in stand houden.

Serverbeveiliging

De serveroplossingen van Dell, uitgerust met geïntegreerde beveiligingsmaatregelen zoals Dell Trusted Server-technologie, bestaan onder andere uit:

- **Root of Trust-hardware:** deze functie zorgt ervoor dat de hardwarecomponenten van de server worden geverifieerd tijdens het opstarten, waardoor er sprake is van een fundamentele beveiligingslaag tegen sabotage of ongeautoriseerde wijzigingen.
- **Ingebouwde beveiligingsfuncties:** Dell-servers zijn uitgerust met zelfversleutelende schijven en end-to-end opstartverificatie, die beschermen tegen ongeautoriseerde toegang en vertrouwen in de integriteit van data wekken.
- **Cybertolerantie:** de aanpak bestaat uit mogelijkheden om afwijkingen, lekken en ongeautoriseerde activiteiten te detecteren, zodat organisaties snel kunnen herstellen van cyberincidenten.
- **Uitgebreide databescherming:** de Trusted Server-oplossingen van Dell zijn voorzien van geïntegreerde beveiligingsmechanismen die data in rust en tijdens overdracht beschermen. Denk hierbij aan geavanceerde versleutelingstechnieken en geautomatiseerde herstelopties om de bedrijfscontinuïteit te garanderen.

Deze mogelijkheden zorgen ervoor dat servers bestand zijn tegen pieken in het dataverkeer en tegelijkertijd de operationele stabiliteit in stand houden. Storageoplossingen beschermen de beschikbaarheid en integriteit van kritieke data tijdens een aanval, waardoor onderbrekingen tot een minimum worden beperkt.

Beveiliging van storage

Dell Storage beschermt tegen DDoS-aanvallen via verschillende geïntegreerde beveiligingsmaatregelen en geavanceerde technologieën die zijn ontworpen om beveiligingslekken te minimaliseren, bedreigingen vroegtijdig te detecteren en snel herstel te garanderen als er een aanval plaatsvindt. Belangrijke methoden zijn onder meer:

- **Proactieve detectie van bedreigingen:** Dell storageoplossingen maken gebruik van intelligente bewakingsfuncties en AI-gestuurde detectie van afwijkingen om ongebruikelijke toegangspatronen te identificeren die kunnen wijzen op een DDoS-aanval. Deze tools bieden realtime beveiligingsinzichten en kunnen geautomatiseerde dreigingsreacties activeren om de impact van een aanval te beperken
- **Root of Trust-architectuur:** deze architectuur is geïntegreerd in storagecontrollers en zorgt voor authenticiteit van de firmware en voorkomt ongeautoriseerde wijzigingen, waardoor de beveiliging van de storagehardware wordt verbeterd en de kans op schendingen tijdens een DDoS-aanval wordt verkleind
- **Multi-factor verificatie (MFA) en toegangscontroles:** dankzij de implementatie van MFA en Role-Based Access Control (RBAC) wordt ongeautoriseerde toegang tot storagesystemen voorkomen, waardoor u nog beter beschermd bent tegen DDoS-aanvallen
- **Micro-segmentatie en netwerkisolatie:** door storagesystemen te isoleren en de toegang tussen workloads te beperken, minimaliseert Dell potentiële aanvalsvectoren en beschermt Dell storagesystemen tegen laterale dataverplaatsing in het geval van een lek
- **Beveiligde snapshots en onveranderlijke logboeken:** de storageoplossingen van Dell bieden veilige snapshots en onveranderlijke logboeken die data-integriteit garanderen zodat organisaties snel kunnen herstellen van DDoS-aanvallen. Deze functies vergemakkelijken forensische analyse van en onderzoek naar incidenten, zodat IT-teams aanvalsvectoren kunnen detecteren en analyseren
- **Cyber Recovery Vault:** oplossingen zoals Dell PowerMax en PowerProtect Cyber Recovery Vault maken air-gapped back-ups. Deze zijn onveranderlijk en zijn beschermd tegen ransomware en andere aanvallen. Deze back-ups kunnen worden teruggeplaatst om de bedrijfscontinuïteit te garanderen zonder risico te lopen opnieuw te worden geïnfecteerd

Door deze uitgebreide beveiligingsfuncties en -technologieën te integreren, beschermen Dell Storage en cybertolerantie organisaties effectief tegen DDoS-aanvallen en houden ze veerkrachtige en veilige IT-omgevingen in stand.

Proactieve bewaking met CrowdStrike

Realtime bewaking en geavanceerde analytics zijn essentieel om abnormale verkeerspatronen vóór escalatie te detecteren. CrowdStrike wordt geïntegreerd in het ecosysteem van Dell om gedragsanalyse en door AI aangedreven inzichten in te zetten om legitieme activiteiten te onderscheiden van aanvalsverkeer, waardoor snel herstel mogelijk is.

Dell PowerProtect voor data-integriteit

Dell PowerProtect zorgt ervoor dat kritieke data veilig en toegankelijk blijven tijdens een DDoS-aanval. Met mogelijkheden om verminking van back-ups te voorkomen en herstelomgevingen te isoleren van de rest van het netwerk kunnen bedrijven systemen worden hersteld en downtime na een incident tot een minimum worden teruggebracht.

Geavanceerde netwerkbeveiliging en microsegmentatie met Dell PowerSwitch Networking en SmartFabric OS

Versterkt de bescherming tegen zero-day-aanvallen dankzij geavanceerde netwerksegmentatie, strikte toegangscontroles en realtime verkeersanalyse in uw hele infrastructuur.

Implementatie in de praktijk

Een wereldwijd e-commerce-platform maakte onlangs gebruik van de PowerProtect-oplossingen van Dell naast proactieve detectiemogelijkheden om een geavanceerde DDoS-aanval af te slaan. Door kritieke systemen te isoleren en noodherstelprocessen te implementeren, kon het bedrijf de volledige activiteiten in recordtijd hervatten, financiële verliezen beperken en het vertrouwen van de klant behouden.

De meerlaagse beveiligingsaanpak

Een succesvolle verdediging tegen DDoS-aanvallen is mogelijk dankzij een gelaagde en adaptieve aanpak. Dell pleit voor de volgende strategieën als aanvulling op zijn technologische aanbod:

Belangrijke stappen om uw verdediging te verbeteren

- **Zero-Trust-architectuur** Implementeer een 'never trust, always verify'-model om elke gebruiker en elk apparaat onder de loep te nemen
- **Geavanceerde versleuteling** versleutelt communicatie op alle lagen om gevoelige gegevens te beschermen die tijdens mogelijke aanvalspogingen worden verzonden.
- **Training voor werknemers** Informeer werknemers over het identificeren van verdachte activiteiten en het volgen van veilige protocollen om onbedoelde inbreuken te voorkomen.
- **Regelmatige systeemtests** Voer routinematige beoordelingen uit, waaronder penetratietests en belastingstests, om de gereedheid van het systeem voor grote verkeersvolumes te beoordelen.

Deze acties, in combinatie met oplossingen van Dell Technologies, zorgen voor een robuust verdedigingsmechanisme tegen geavanceerde bedreigingen.

Partnerschappen die cyberbeveiliging versterken

Dell Technologies werkt samen met marktleiders zoals **Microsoft**, **CrowdStrike** en **Secureworks** om de mogelijkheden uit te breiden. Deze partnerschappen bieden extra beschermingslagen, waarbij de beste dreigingsinformatie en geavanceerde detectiemethodieken worden opgenomen in het uitgebreide framework van Dell.

Dell Professional Services benutten

Naast technologie zorgt Dell Professional Services voor deskundige begeleiding aan bedrijven die te maken hebben met DDoS-uitdagingen. Het team van Dell zorgt ervoor dat organisaties snel kunnen herstellen en toekomstige verdediging kunnen versterken - van incidentrespons tot advies over beveiligingsarchitectuur op maat.

Een veerkrachtige toekomst opbouwen

Dell Technologies is meer dan een technologieleverancier. Dell is een partner die zich inzet om uw bedrijf te beschermen tegen de veranderende dreiging van DDoS-aanvallen. Door geavanceerde technologie, diepgaande partnerschappen en uitvoerbare inzichten te combineren, helpt Dell bedrijven hun activiteiten te beschermen, het vertrouwen van klanten te behouden en actief groei na te streven.

Zet vandaag nog de eerste stap naar veerkracht. Neem contact op met Dell Technologies om uw bedrijf te beter tegen DDoS-bedreigingen te beschermen en uw toekomst te veilig te stellen.

Dell Technologies stelt bedrijven in staat om de uitdagingen van DDoS-cyberbeveiliging te overwinnen, wat bewijst dat een veilige basis de sleutel is tot succes in een onderling verbonden wereld.

Ontdek op **Dell.com/SecuritySolutions** hoe u enkele van de grootste uitdagingen op het gebied van cyberbeveiliging van dit moment kunt aanpakken

Meer informatie over Dell oplossingen

Neem contact op met een Dell Technologies Expert

Bekijk meer informatiebronnen

Neem deel aan het gesprek via #HashTag

DELL Technologies